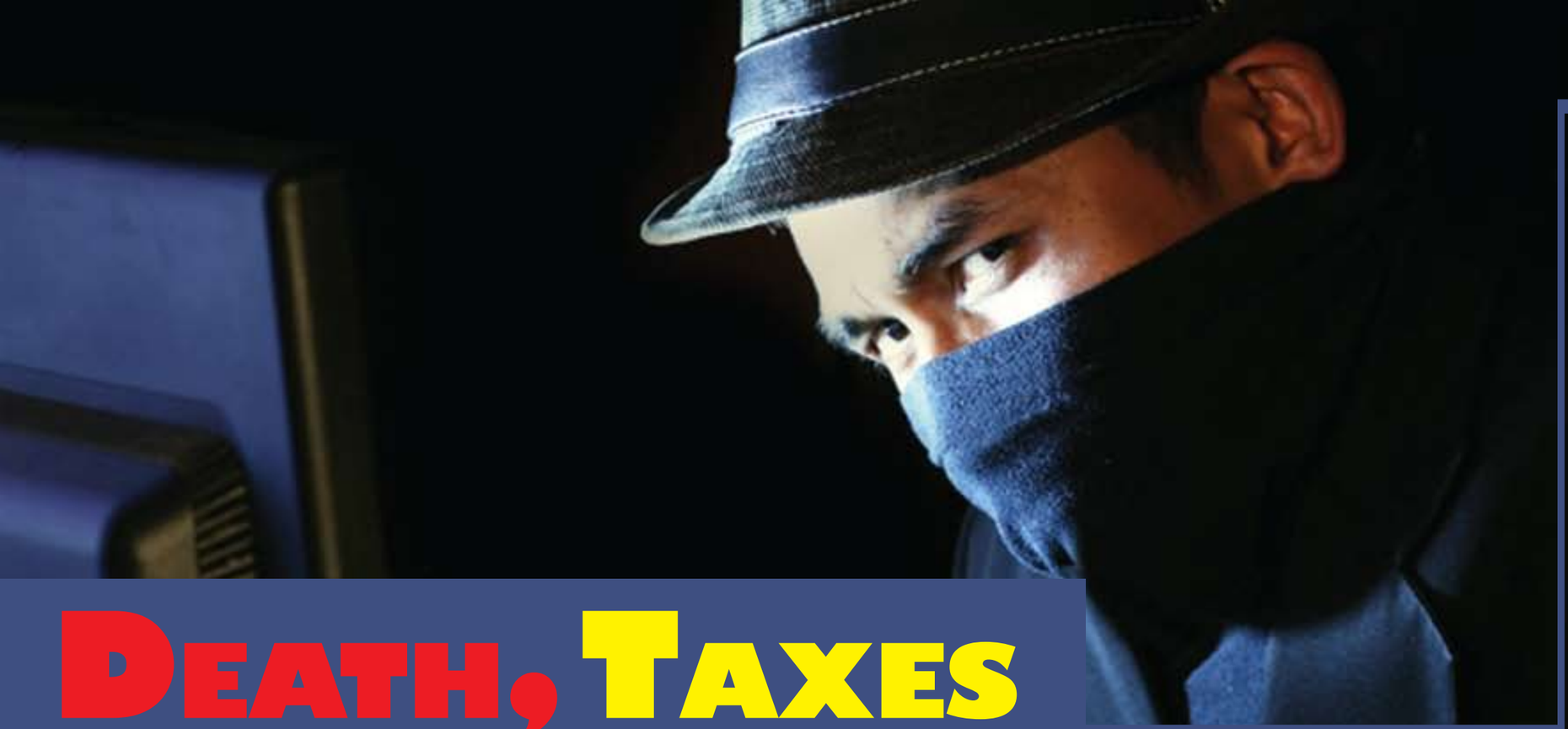

Death, Taxes and Cybercrime

The mortgage industry as a whole has been slow to adopt standards for fighting cybercrime, but in fairness, so have many businesses.

If Benjamin Franklin were writing today, we would no doubt see an updated version of his famous saying that would read, "In this world nothing can be said to be certain, except death, taxes – and cybercrime." He would have been blogging, tweeting and Facebooking, and would certainly have understood that the pervasive reality of computers in modern life would inevitably lead to their misuse. Mortgage lenders are just starting to get a taste of cybercrime, but can expect more.

By Bill Mitchell

Cybercrime is defined broadly as any illegal activity using computers. Since computers are now literally everywhere from our pockets to our running shoes, no one is safe from fraud and other crimes involving technology. The temptation for criminals is simply too great: there are almost unlimited possibilities for mischief stored on the world's computers and for people with the right skills, the information is there for the taking.

The FBI's cybercrime web page poses an intriguing question: "We are building our lives around our wired and wireless networks. The question is, are we ready to work together to defend them?" Are we? It is a probing question that makes one realize how little we know about the true potential for becoming victims. Moreover, it raises questions about the mortgage industry's exposure and what is being done to safeguard borrower information.

Consider the attacks we have seen in the fairly recent past from criminals seeking consumer financial information:

In 2007, the parent of clothing discounters T.J. Max and Marshalls revealed that its systems had been compromised for more than a year, and that tens of millions of credit and debit card numbers had been stolen. Eleven computer hackers were busted for the theft, but the long-term damage is yet to be determined.

In 2008, the Bank of New York Mellon put ten backup data tapes into a truck and sent them to a storage facility. Only nine arrived, and the missing tape, incredibly unencrypted like the rest, happened to contain bank accounts and social security numbers for 4.5 million bank customers.

Also in 2008, the Hannaford Brothers grocery chain in Maine disclosed that the company's systems had been the victim of a cyber invasion, with the criminals obtaining access to 4.2 million credit card transactions. Over 1,800 of the card numbers were used to obtain cash at Hannaford stores before the theft was discovered. The company had recently undergone a PCI (Payment Card Industry) assessment, too, but it didn't prevent the security breach.

The message is clear for consumers: no matter where you are and what you are doing – or even if you are doing nothing at all – your personal information and accounts are under attack. A great deal of financial cybercrime is small-time, involving dozens, hundreds or thousands of accounts. The jackpot for hackers happens when they can breach significant repositories containing hundreds of thousands or even millions of account numbers. The viable accounts are promptly sold to bolder culprits who create further havoc for victims from there. According to the U.S. Treasury Department, attacks are happening on American defense and financial institutions 24/7, often from locations in Russia and countries of the former Soviet Union, and China.

"People often ask how much of a threat this is," said former Homeland Security Secretary Michael Chertoff. "It's not a threat – it's actually happening." Though estimates of the scope of cybercrime differ, Chertoff's consulting firm says that cybercriminals have actually exceeded the annual dollar volume of the global drug trade, citing the staggering figure of $100 billion. For reference, think of an entire

bedroom of your home filled with stacks of $100 bills. Now picture a hundred such rooms. That's a lot of portraits of wise Ben Franklin.

But the actual cost could be more than we know. One of the most important studies on cybercrime came from the Ponemon Institute in August of 2011. The study, sponsored by HP's ArcSight, a cyber security solutions provider, found that the median cost of cybercrime increased by 56 percent over the previous year and now costs the 50 U.S. based businesses surveyed an average of $6 million per year, mainly in prevention costs. Perhaps of most concern is the study's comment that many companies decline to report cybercrime for a variety of understandable reasons. The implication that the problem is actually far greater than previously thought is disturbing.

What can the mortgage industry do to safeguard against cybercrime? As an LOS provider, Mortgage Builder has been watching this developing threat for years. CEO Keven Smith had strong opinions early on about protecting client data and had the company covered by a relatively new type of policy called "cyber liability insurance," or CLI. With SaaS and cloud delivery becoming the industry's choice for loan origination software services, lenders entrust far more to their providers these days than in years past.

"We do not consider cyber liability insurance coverage to be an option, it's a necessity," Smith notes. "Cyber criminals have become more sophisticated as the amount of information available in cloud computing environments has grown. It's part of our responsibility to protect it."

Cyber liability coverage is already a requirement for some lenders as they look at new LOS systems, particularly among the nation's community banks. References to cyber threat measures and CLI are appearing more and more frequently in RFPs (Requests for Proposals) among midsize lenders when considering new loan origination software solutions.

Another step that can be taken is something else Mortgage Builder has been doing for a long time: obtaining SAS 70 Type II audit certification. SAS 70 Type II differs from the SAS 70 audit in that actual onsite physical verification of security measures, control objectives and activities has taken place by an independent auditor qualified by the American Institute of Certified Public Accountants. It is another protection against information theft that is not required of LOS companies, but more lenders are looking for it as they seek answers to cybercrime.

The latest version of the SAS 70 Type II is more elaborate, replacing the previous standard with the new SSAE 16 Type II audit. What they lack in naming creativity, they gain in points for thoroughness – it is not a trivial achievement to pass muster with these auditors. Even after nine consecutive successes, we find that it takes attention to detail and significant preparation, which is exactly the sort of precision needed to protect sensitive borrower information.

The mortgage industry as a whole has been slow to adopt standards for fighting cybercrime, but in fairness, so has the rest of the business world. Never a concern on a big scale until recently, the problem's scope is yet to be fully understood. Just when it seems possible to grasp the most serious threats to data security, a new one pops up from an unexpected source. The cybercriminals know no geographic boundaries – that much we know. As the Department of Defense has found, they also seem to have no limits on innovation; as soon as one backdoor virus is found and countered, another surfaces to take its place.

As technology professionals, it is up to us to provide safety and security for those we serve to the best of our ability. Like death and taxes, cybercrime is the new certainty. ❖

About The Author

Bill Mitchell is Vice President and National Sales Manager for Mortgage Builder Software. With 20 years of technology experience, he is responsible for planning, execution and delivery in Mortgage Builder's nationwide sales effort. Mortgage Builder has been providing industry leading loan origination solutions to credit unions, CUSOS, community banks, mortgage bankers and other financial institutions since 1998. Bill can be reached at Bill.Mitchell@MortgageBuilder.com.

Index of Advertisers